

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1514173-000

Total Deleted Page(s) = 1  
Page 2 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXX

- 1 -

FEDERAL BUREAU OF INVESTIGATION

b6  
b7C  
OTHER Sealed

Date of transcription 03/02/2011

On March 2, 2012, [REDACTED]

[REDACTED]

All [REDACTED] records are maintained in UTC, which is the same as GMT for time zone purposes. Any fields that are blank or OTHER Sealed any files that have no content between the PGP header and signature block indicate that there are no responsive records.

The zip files were burned to CDROM and the CDROM is maintained in the 1A section of the file.

[REDACTED] was forwarded to SA [REDACTED] on March 2, 2012.

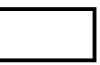
b6  
b7C  
OTHER Sealed

Investigation on 03/02/2012 at Salt Lake City, Utah

File # [REDACTED] Date dictated                     

by SA [REDACTED]

b6  
b7C  
b7E





U.S. Department of Justice

Federal Bureau of Investigation

In Reply [redacted]  
File No. [redacted]

257 East 200 South  
Suite 1200

March 5, 2012

b7E



Dear Custodian of Records:

A criminal investigation is being conducted by the Federal Bureau of Investigation into violations of federal law. You are requested to preserve all records including [redacted]



b7E



This preservation of evidence notice is given pursuant to Title 18 USC Section 2703(f), while our office obtains necessary legal process. Please contact Intelligence Analyst [redacted] telephone number [redacted] [redacted] with any questions.

b6  
b7C  
b7E

Sincerely,

David J. Johnson  
Special Agent in Charge

By: [redacted]

[redacted]  
Supervisory Special Agent

b6  
b7C

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1514173-000

Total Deleted Page(s) = 6

Page 1 ~ b6; b7C; b7E;

Page 2 ~ b7E;

Page 3 ~ b7E;

Page 4 ~ b6; b7C; b7E;

Page 5 ~ b6; b7C; b7E;

Page 6 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

X Deleted Page(s) X

X No Duplication Fee X

X For this Page X

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1514173-000

Total Deleted Page(s) = 43

Page 1 ~ OTHER - Sealed Pursuant to Court Order;  
Page 2 ~ OTHER - Sealed Pursuant to Court Order;  
Page 3 ~ OTHER - Sealed Pursuant to Court Order;  
Page 4 ~ OTHER - Sealed Pursuant to Court Order;  
Page 5 ~ OTHER - Sealed Pursuant to Court Order;  
Page 6 ~ OTHER - Sealed Pursuant to Court Order;  
Page 7 ~ OTHER - Sealed Pursuant to Court Order;  
Page 8 ~ OTHER - Sealed Pursuant to Court Order;  
Page 9 ~ OTHER - Sealed Pursuant to Court Order;  
Page 10 ~ OTHER - Sealed Pursuant to Court Order;  
Page 11 ~ OTHER - Sealed Pursuant to Court Order;  
Page 12 ~ OTHER - Sealed Pursuant to Court Order;  
Page 13 ~ OTHER - Sealed Pursuant to Court Order;  
Page 14 ~ OTHER - Sealed Pursuant to Court Order;  
Page 15 ~ OTHER - Sealed Pursuant to Court Order;  
Page 16 ~ OTHER - Sealed Pursuant to Court Order;  
Page 17 ~ OTHER - Sealed Pursuant to Court Order;  
Page 18 ~ OTHER - Sealed Pursuant to Court Order;  
Page 19 ~ OTHER - Sealed Pursuant to Court Order;  
Page 20 ~ OTHER - Sealed Pursuant to Court Order;  
Page 21 ~ OTHER - Sealed Pursuant to Court Order;  
Page 22 ~ OTHER - Sealed Pursuant to Court Order;  
Page 23 ~ OTHER - Sealed Pursuant to Court Order;  
Page 24 ~ OTHER - Sealed Pursuant to Court Order;  
Page 25 ~ OTHER - Sealed Pursuant to Court Order;  
Page 26 ~ OTHER - Sealed Pursuant to Court Order;  
Page 27 ~ OTHER - Sealed Pursuant to Court Order;  
Page 28 ~ OTHER - Sealed Pursuant to Court Order;  
Page 29 ~ OTHER - Sealed Pursuant to Court Order;  
Page 30 ~ OTHER - Sealed Pursuant to Court Order;  
Page 31 ~ OTHER - Sealed Pursuant to Court Order;  
Page 32 ~ OTHER - Sealed Pursuant to Court Order;  
Page 33 ~ OTHER - Sealed Pursuant to Court Order;  
Page 34 ~ OTHER - Sealed Pursuant to Court Order;  
Page 35 ~ OTHER - Sealed Pursuant to Court Order;  
Page 36 ~ OTHER - Sealed Pursuant to Court Order;  
Page 37 ~ OTHER - Sealed Pursuant to Court Order;  
Page 38 ~ OTHER - Sealed Pursuant to Court Order;  
Page 39 ~ OTHER - Sealed Pursuant to Court Order;  
Page 40 ~ OTHER - Sealed Pursuant to Court Order;  
Page 41 ~ OTHER - Sealed Pursuant to Court Order;  
Page 42 ~ OTHER - Sealed Pursuant to Court Order;  
Page 43 ~ OTHER - Sealed Pursuant to Court Order;

XXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXX

**This second page contains personal identifiers provided for law-enforcement use only  
and therefore should not be filed in court with the executed warrant unless under seal.**

*(Not for Public Disclosure)*

Name of defendant/offender: \_\_\_\_\_

Known aliases: \_\_\_\_\_

Last known residence: \_\_\_\_\_

Prior addresses to which defendant/offender may still have ties: \_\_\_\_\_

Last known employment: \_\_\_\_\_

Last known telephone numbers: \_\_\_\_\_

Place of birth: \_\_\_\_\_

Date of birth: \_\_\_\_\_

Social Security number: \_\_\_\_\_

Height: \_\_\_\_\_ Weight: \_\_\_\_\_

Sex: \_\_\_\_\_ Race: \_\_\_\_\_

Hair: \_\_\_\_\_ Eyes: \_\_\_\_\_

Scars, tattoos, other distinguishing marks: \_\_\_\_\_

History of violence, weapons, drug use: \_\_\_\_\_

Known family, friends, and other associates (*name, relation, address, phone number*): \_\_\_\_\_

FBI number: \_\_\_\_\_

Complete description of auto: \_\_\_\_\_

Investigative agency and address: \_\_\_\_\_

Name and telephone numbers (office and cell) of pretrial services or probation officer (*if applicable*): \_\_\_\_\_

Date of last contact with pretrial services or probation officer (*if applicable*): \_\_\_\_\_

JOHN ANTHONY BORELL III,  
the defendant herein, knowingly caused the transmission of a program,  
information, code and command, and as a result of such conduct, intentionally  
caused damage without authorization, to a protected computer, to wit: he did  
compromise the server(s) hosting the website <http://www.utahchiefs.org> using a  
program called "Havij"; and the offense caused loss to one or more persons during  
a one-year period aggregating at least \$5,000; all in violation of  
18 U.S.C. §1030(a)(5)(A).

COUNT 2

On or about January 31, 2012, in the Central Division of the District of  
Utah,

JOHN ANTHONY BORELL III,  
the defendant herein, knowingly caused the transmission of a program,  
information, code and command, and as a result of such conduct, intentionally  
caused damage without authorization, to a protected computer, to wit: he did  
compromise the server(s) hosting the website <http://slcpd.com> using a program  
called "Havij"; and the offense caused loss to one or more persons during a one-  
year period aggregating at least \$5,000; all in violation of

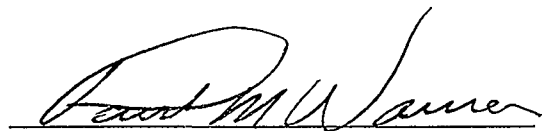
18 U.S.C. §1030(a)(5)(A).

Complainant states that this complaint is based on information obtained through investigation consisting of the following:

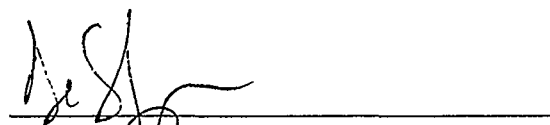
See Sealed Affidavit, attached and incorporated herein by reference.

  
ERIC ZIMMERMAN  
Special Agent, F.B.I.

Sworn to and subscribed before me  
on this 16<sup>th</sup> day of March, 2012.

  
PAUL M. WARNER  
United States Magistrate Judge

Approved:

  
ADAM ELGGREN  
Assistant U.S. Attorney



**SEALED AFFIDAVIT OF ERIC ZIMMERMAN IN SUPPORT OF**

**CRIMINAL COMPLAINT**

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since October 1, 2007. Currently, I am assigned to the Cyber Crime Squad of the Salt Lake City, Utah Field Office.

The facts in this affidavit come from my personal observations, my training and experience and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the complaint and does not set forth all of my knowledge about this matter as they relate to violations of Title 18 United States Code (U.S.C.) §1030(a)(5)(A), Fraud and Related Activity in Connection with Computers. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code (U.S.C.) §1030(a)(5)(A), Fraud and Related Activity in Connection with Computers, have been committed by an individual named John Anthony Borell III.

2. My experience as an FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud and intrusion. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, intellectual property and other computer-based crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally

participated in the execution of search warrants involving the search and seizure of computer equipment as well as interview and interrogation of subjects in regards to cyber crimes.

### **Summary of Relevant Computer and Internet Concepts**

3. The Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even where the two computers are located in the same state.

4. The term 'computer', as used herein, is defined pursuant to Title 18 USC § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." A "protected computer" (18 U.S.C. §1030(e)(2)) is a computer used in or affecting interstate or foreign commerce or communication.

5. Internet Service Providers ("ISPs"): Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). Xfinity, Microsoft ("MSN"), and Qwest are examples of some of the larger and better-known ISPs. Other ISPs include private entities such as corporations, universities, and government agencies. Among other services, ISPs provide their customers with access to the Internet using telephone, cable, Digital Subscriber Line ("DSL"), or other types of telecommunications lines.

6. Internet Protocol Address (“IP address”): An Internet Protocol (“IP”) address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet service providers assign IP addresses to their customers’ computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called “dynamic IP addressing”), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called “static IP addressing”). Either way, the IP address used by a computer attached to the Internet must be unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customers’ connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

#### **TWITTER, INC.**

7. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

8. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

9. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

10. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

11. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

12. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other

users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have favorited or retweeted the user’s own Tweets, as well as a list of all Tweets that include the user’s username (*i.e.*, a list of all “mentions” and “replies” for that username).

13. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

14. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

15. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter’s link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

16. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right

side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

17. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

18. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

19. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

20. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

21. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

22. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

23. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

### **FACTS SUPPORTING PROBABLE CAUSE**

#### **BACKGROUND INFORMATION**

24. Based on FBI investigation, your affiant knows that the hacktivist (hacker-activist) network Anonymous is a loose affiliation of individuals spanning the world. Anonymous has no defined leadership or membership and anyone is invited to act in the name of Anonymous. As a result, Anonymous itself is more a movement or idea than an organization. In practice, the label Anonymous is the banner under which individuals and groups commit actions—including intrusions into computer systems. One of these groups is known as CabinCr3w.

25. CabinCr3w is a defined group of individuals, two of whom use the Twitter accounts @ItsKahuna and @Anonw0rmer, who associate and conspire to differing levels to hack computer systems. CabinCr3w specifically targets law enforcement agencies, non-governmental organizations associated with law enforcement, and the personal lives of those who work in law enforcement related fields. While CabinCr3w is a distinct and definable group of individuals, their activities are justified by the concept of Anonymous, and their activities are ascribed thereto.

26. On February 15, 2012, your affiant reviewed logs from various Internet Relay Chat (IRC) channels looking for any references to 'Kahuna.' Users on IRC can switch their nicknames by issuing a command to the server. When a user changes his nickname, the server will report the old nickname and the new nickname of the user to let other IRC users know the nickname change has occurred. Several other nicknames used by Kahuna were found to include: specter, anonjb, crypto667, m15t1k, and vector.

27. On February 15, 2012, your affiant searched various FBI databases and found two documents which contained a reference to the nickname 'anonjb.'

28. Both documents summarize information received from someone claiming to be John Anthony Borell III. Two tips were made on or about August 25, 2011, one via tips.fbi.gov and one via ic3.gov. Both tips originated from 174.159.183.198 which resolves to Sprint Nextel Corporation.

29. Both tips were identical and stated that Borell is a member of AntiSec (AntiSec is an abbreviation for Anti-Security) as well as Anonymous, and goes by the nicknames Specter\_, Kahuna, TehTiger, and anonJB. The tips provided the following address for Borell:



[redacted] Toledo, Ohio 43612. Borell's telephone number is 419-787-8231. The tips provided an email address of jborell3@gmail.com. The tips stated Borell has participated in numerous government agency intrusions as well as the leaking of classified documents. Borell was active in anonops (Anonymous operations) and has aided in the hacking of multiple individuals as well. The tips further claimed that Borell was the lead in the Satiagraha leaks of Brazilian files and hosted them on his website, satiagrahaleaks.org, and had been in contact with Sabu (Sabu is the leader of Lulzsec, a hacking group affiliated with Anonymous). Finally, the tips stated Borell has knowledge of the group's (Anonymous) inner workings and has trusted relationships with many of the members. Borell claimed he was tired of running and hiding.

b6  
b7C

30. Your affiant conducted additional database searches for John Borell and found a reference to another FBI case. Your affiant reviewed the information in the case file.

31. One of the documents in the case file contained a link to <http://pastie.org/2477266> which shows registration details for <http://satiagrahaleaks.org/> as belonging to John Borell III, [redacted] Toledo, Ohio with phone number 419-787-8231.

b6  
b7C

32. Another document in the case contains details about a computer intrusion which originated from IP address 72.240.43.146. Subpoena information shows the subscriber for this IP address as Blessed Sacrament Parish, located at [redacted] Toledo, Ohio 43613.

b6  
b7C

33. On February 6, your affiant searched Google for various iterations of jborell3@gmail.com.

34. A Facebook profile was located at <https://www.facebook.com/Jborell>. Borell's Facebook page has a profile picture which was taken via cell phone while Borell looked into a mirror. Additional information on his profile indicates he went to Sylvania Northview High

School and lives in Sylvania, Ohio. The profile picture on this Facebook account matches Borell's driver's license photo, which your affiant has viewed from the records of the Ohio Department of Motor Vehicles.

35. A Twitter profile was found at <http://twitter.com/#!/Jborell3>. Borell's Twitter page has a profile picture which is a cropped version of his Facebook profile image. This Twitter account was last updated on July 14, 2011 at 11:22 AM. Several tweets of interest were found to include:

- a. Borell responding to a tweet from @LulzSec on June 22, 2011 at 12:54 PM
- b. Borell retweeting a tweet from @YourAnonNews on June 21, 2011 at 8:24 AM
- c. Borell tweeted "<http://bit.ly/kiRjOt> ---Sort of Tempted" on June 26, 2011 at 09:58 AM which redirects to <http://thehackernews.com/2011/06/microsoftcom-server-vulnerable-to.html> which contains the statements: "A hacker with Codename "No.One" release some vulnerability regarding DOLE via a pastebin<sup>1</sup> post. We analyse it & Explaining the possible Security Breach." The vulnerabilities discussed on this webpage relate to SQL injections (the hacking technique alleged to have been used by Borell; see para. 60 below).
- d. Borell tweets about switching to Sprint for his cell phone carrier on June 9, 2011 at 8:42 PM.

---

<sup>1</sup> Pastebin.com is a website where text can be stored online for a set period of time. Pastes may be public or private. Public pastes are viewable by all Pastebin.com visitors, while private pastes are invisible unless the paster shares his/her private link. Pastebay.net provides the same type of service as pastebin.com.

36. A YouTube profile was found at <http://www.youtube.com/user/jborell3>. The latest activity on the account was on January 12, 2012. The profile has a link to "What is Anonymous? What is "The Plan"? <http://www.youtube.com/watch?v=Drx8cwG-aKE>" which was added six months ago.

37. A pastebin post titled "Kahuna Pentagon Leak Log" was found at <http://pastebin.com/xSmnHZZp>. The post was created on January 29, 2012. The post contains several sections of IRC logs between Kahuna and others.

38. The log file at <http://pastebin.com/xSmnHZZp> for August 27, 2011 contains:

(12:41:09)<Kahuna> This is super relaxing, im doing some IT work at a church i help with computer stuff at and there is a sting quartet practicing a room away - 15 min, 23 sec  
(12:56:32)<Presstorm> how big was that brazil leak again?  
(12:56:34)<Presstorm> 50 GB?  
(12:57:24)<Kahuna> 5gb  
(12:57:37)<Presstorm> ok  
(12:57:47)<Kahuna> I wish it was 50  
(12:57:48)<Kahuna> damn  
(19:11:20)<Kahuna> I talked to my lawyer, the benefit of having a father as an attorney is i have connections  
(19:11:25)<Kahuna> he will be representing me  
(19:11:52)<Kahuna> He said when the FBI shows up dont tell them anything and give them his card and tell them if they need to talk they should go through him  
(19:12:13)<Kahuna> And i wont be speaking till they contact the district attorney's office and get a full grant of immunity  
(19:14:04)<Kahuna> I told him i wont be giving up anyone  
(19:14:05)<Kahuna> even if they try to charge me

39. A search for lawyers in Ohio was conducted at <http://www.ohiobar.org/Pages/FindALawyer.aspx?Names=john&LastName=borell&ZipCode=&TypeOfLawyer=-1&pn=1>. Two lawyers named John Borell were located:

Name: John Anthony Borell Esq.  
Firm: Lucas County Prosecutors Office  
Address: 700 Adams St Ste 250

Assistant Prosecuting Attorney  
Toledo, Ohio 43604-5659  
(419) 213-4728

Name: John Anthony Borell Esq.  
Firm: Marshall & Melhorn, LLC  
Address: 4 SeaGate 8th Fl  
Toledo, Ohio 43604-1599  
(419) 249-7166

### SEARCH WARRANT AND SUBPOENA INFORMATION

40. On February 17, 2012, a search warrant was sent to Twitter for the following Twitter accounts: @ItsKahuna, @Anonw0rmer, and @cabincr3w. On March 2, 2012, Twitter provided information for the above accounts pursuant to the search warrant. Included in the search warrant return was information related to IP addresses used by the accounts, all Twitter messages sent using the accounts, direct messages sent to and from the accounts, and basic user information for the accounts, such as the email address that created the account.

41. On March 5, 2012, a grand jury subpoena was sent to Buckeye Telesystems for several IP addresses found in the Twitter search warrant return related to ItsKahuna: 72.240.142.167, 72.241.1.22, 72.240.137.223, and 72.240.43.146.

42. On March 6, 2012, Buckeye Telesystems responded to the subpoena and provided subscriber information for each IP address as follows:

43. 72.240.142.167 is subscribed to by an individual with the initials P. M., located at  Toledo, Ohio 43612. This IP address was assigned dynamically, meaning there is a possibility of it changing over time. While an IP is assigned to a particular customer, it is considered leased. The lease for IP address 72.240.142.167 was obtained on 06/13/2011 at 11:47 AM EST and expired on 03/01/2012 at 10:29 PM EST.

b6  
b7c

44. [REDACTED] is approximately 312 feet from [REDACTED] Toledo, Ohio which is a known address for Borell to include the address on his driver's license.

b6  
b7c

45. On Thursday, December 22, 2011 at 4:49:00 PM EST, ItsKahuna tweeted the following: "Neighbors I thank you for installing a new router today and choosing WEP to protect it. I much appreciate the extra bandwidth for torrents."

46. On Tuesday, February 28, 2012 at 7:48:00 PM EST, ItsKahuna tweeted the following: "Neighbors thank you for having WEP on your router and amazing dl speeds, im quite enjoying it atm."

47. The IP audit file from the Twitter search warrant return related to ItsKahuna shows three sessions being initiated with Twitter which were created on Tuesday, February 28, 2012 from IP address 72.240.142.167: 8:37:29 AM EST, 8:53:25 PM EST, and 9:49:27 PM EST.

48. The IP audit file from the Twitter search warrant return related to ItsKahuna shows three sessions being initiated with Twitter which were created on Wednesday, February 29, 2012 from IP address 72.240.142.167: 1:51:43 PM EST, 4:51:44 PM EST, and 6:32:15 PM EST.

49. During the course of this investigation, your affiant obtained a driver's license photo of John Anthony Borell III from the state of Ohio. This photo was sent to agents in Ohio who were conducting surveillance of the addresses Borell was thought to be using.

50. On March 7, 2012 at 8:24 AM EST, John Anthony Borell III was observed exiting [REDACTED] and getting into a red Dodge Daytona with OH license plate FJV7951. This vehicle drove to 5656 Opportunity Drive which is located in Toledo, Ohio. The vehicle was

b6  
b7c

parked directly between Affinity Information Management (AIM) and another business in the center of the parking lot. This same license plate has been seen in the same area of the parking lot at 5656 Opportunity on or around February 29, 2012. 5656 Opportunity Drive is the address for AIM.

51. Ohio plate FJV7951 comes back to a 1989 Dodge Daytona with VIN 1B3XG24K2KG205199. The vehicle is currently registered to Ian M Shaw, date of birth [REDACTED] [REDACTED] with the address [REDACTED] Sylvania, Ohio 43560-1869.

b6  
b7c

52. This address is the same as the subscriber information for IP address 72.241.1.22.

53. On December 17, 2011 at 8:22 PM EST, ItsKahuna tweeted the following:

@dwill6413 Im not on my computer, i would never us ubuntu. Fixing a friends

54. The IP audit file from the Twitter search warrant return related to ItsKahuna shows a session being initiated with Twitter which was created on December 17, 2011 at 7:55:59 PM EST from IP address 72.241.1.22.

55. Ian Shaw's Facebook page is <https://www.facebook.com/people/Ian-Shaw/1806903320?sk=info>. One of Ian Shaw's friends on Facebook is John Borell III whose Facebook page is <https://www.facebook.com/Jborell>.

56. 72.241.1.22 is subscribed to by John Shaw, located at [REDACTED] Sylvania, Ohio 43560. This IP address was assigned dynamically. The lease was obtained on 03/15/2011 at 2:54 AM EST and expired on 03/06/2012 at 14:43 PM EST.

b6  
b7c

57. 72.240.137.223 is subscribed to by Affinity Information Management, located at 5656 Opportunity Drive, Suite 11 Toledo, Ohio 43612. This IP address was assigned

dynamically. The lease was obtained on 11/10/2011 at 8:53 AM EST and expired on 03/06/2012 at 11:56 PM EST.

58. On March 8, 2012, John Borell and Ian Shaw were observed in the Dodge Daytona mentioned above pulling into the AIM parking lot. Both Borell and Shaw exited the vehicle and entered AIM at 8:30 AM EST.

59. 72.240.43.146 is subscribed to by Blessed Sacrament Church, located at 4227 Bellevue Road, Toledo, Ohio 43613-3936. This IP address is static which means it does not ever change.

## HACKING EVENTS

### Utahchiefs.org

60. On January 19, 2012, the computer servers that host the website <http://www.utahchiefs.org> (UC) were compromised. This website is a publicly-accessible website used by current and former chiefs of police to communicate, and contains a great deal of private, non-publicly accessible information. Your affiant reviewed the UC web server log files and found 44775 log entries for IP address 72.240.137.223. This IP was first seen on 01/19/2012 08:25:34 AM MST and last seen on 01/19/2012 04:43:52 PM MST. IP address 72.240.137.223 resolves to Borell's place of work, AIM, in Toledo, Ohio (see para. 56 above). The attacker used an automated SQL injection tool called 'Havij'<sup>2</sup> to compromise the UC website.

---

<sup>2</sup> Exploiting a SQL (pronounced "sequel") injection involves sending data to a web site which the website was not programmed to handle properly. For example, if a web page requested a person to enter their first and last name and a user does so, things will work as expected. However, if a user enters database specific commands in the first name field, to delete or modify data for example, the web server and database will process the request as it would if a first

61. On January 19, 2012 at 4:11 PM, @ItsKahuna posted a tweet which stated: "Utah Chiefs Of Police Association Hacked #OpMegaupload <http://www.utahchiefs.org> <http://pastebay.com/298247>. Admin Logins Included. Enjoy Comrades."

62. <http://pastebay.com/298247> contains an outline of the Utah Chiefs Of Police Association website hack which includes a list containing the name, email address, and hashed password of approximately 24 chiefs of police from various cities in Utah. The page is signed @ItsKahuna. (note: The URL above is not currently available anymore, but was printed and is maintained in the case file.)

63. On January 19, 2012 at 4:13 PM, @ItsKahuna posted a tweet which stated "Utah Chiefs Of Police Association Admin Login | Username: heather | password: butterfly <http://www.utahchiefs.org>."

---

name was entered. In some cases, the commands can be issued in such a way that the entire database can be exposed to the user sending the illegitimate commands. The following paragraphs further explain SQL injections and how Havij, an automated SQL injection tool, works:

An SQL injection is often used to attack the security of a website by inputting SQL statements (computer language) in a web form to get a poorly designed website to perform operations on the database (often to dump the database content to the attacker) other than the usual operations as intended by the designer. SQL injection is a code injection technique that exploits a security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL commands are thus injected from the web form into the database of an application (like queries) to change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system. The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injecting vulnerable targets using Havij. The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users.



64. On January 19, 2012 at 6:22 PM, @ItsKahuna posted a tweet which stated "Whoever removed the Megaupload image from <http://Utahchiefs.org> and replaced it with their nick when i hacked it for a purpose. Fuck Off."

65. On January 19, 2012 at 6:23 PM, @ItsKahuna posted a tweet which stated "<http://Utahchiefs.org> back down again. Getting Too Much Traffic. I just need it back up for 30 seconds so i can log in and rick<sup>3</sup>roll<sup>3</sup> them all."

66. On January 19, 2012 at 6:27 PM, @ItsKahuna posted a tweet which stated "Whoever is attacking <http://Utahchiefs.org> stop for a few so I can rick roll them all with the admin account email. Kthnx."

67. On January 20, 2012 at 10:58:27 PM GMT, joshloftin (another Twitter user who follows, or is followed by, ItsKahuna) sent a direct message to ItsKahuna which stated "Did you hack <http://t.co/vOzi4SX>? What did you display (screen grabs?) before site went down? Why <http://t.co/vOzi4SX>?" <http://t.co/vOzi4SX> resolves to <http://www.utahchiefs.org>.

68. On January 21, 2012 at 00:09:56 AM GMT, ItsKahuna sent a direct message to joshloftin which stated "I didnt have any screenshots it was going too fast with everythinggoing on. But yes I hacked it. Put up a megavideo logo and small message."

69. On January 21, 2012 at 00:11:31 AM GMT, ItsKahuna sent a direct message to joshloftin which stated "It was at the time an unrelated hack, Just one i was working on but I decided it was a good spot to spread the message about megavideo."

---

<sup>3</sup> "Rick roll" is shorthand for tricking somebody online into viewing something they weren't expecting.

70. The administrator for the Utah Chiefs website estimates \$150,000 in damages accrued in responding to this hacking event.

**Salt Lake City Police Department**

71. On January 31, 2012, administrators of the Salt Lake City Police Department (SLCPD) website noticed three extra pages had been created on the SLCPD website. SLCPD administrators disabled the site after finding the extra pages. Your affiant reviewed the SLCPD web server logs and found over 18,000 connections from IP address 72.240.137.223, the AIM IP address. The vast majority of these connections are SQL injection attempts directed at the servers hosting the SLCPD website. The initial request to the SLCPD website from 72.240.137.223 (the IP address assigned to AIM, where Borell works) was on January 31, 2012 at 8:32:37 AM MST and the last request was on January 31, 2012 at 12:58:53 PM. The attacker used Havij to compromise the SLCPD website.

72. On January 31, 2012 at 1:40 PM, @ItsKahuna posted a tweet which stated "HACKED: <http://slcpd.com> #OpPiggyBank <http://bit.ly/zkaFu3> OVER 1k users/pass | D0x <http://bit.ly/w1wGrH> #Anonymous #CabinCr3w."

73. On January 31, 2012 at 2:13 PM, @ItsKahuna posted a tweet which stated "<http://www.slcpd.com/login.php> Username: amarvel Password: marvel #StaffLogin #OpPiggyBank."

74. On January 31, 2012 at 2:21 PM, @ItsKahuna posted a tweet which stated "SLCPD. Shut Down The Website, But Its Too Late For Damage Control. I Have Your Crime Tip Police Reports. Will Keep Them Safe For You."

75. On January 31, 2012 at 2:23 PM, @ItsKahuna posted a tweet which stated "SLCPD, It Took Utah Chiefs 4 Days To Fix Their Shit. Find Out How I Did It. Tick Tock Tick Tock. Make It A Race. If You Win I Wont Dump More."

76. On January 31, 2012 at 3:43 PM, @ItsKahuna posted a tweet which stated "http://slcpd.com #OpPiggyBank Mirror: [pastebin.net/306596](http://pastebin.net/306596) Pastebin Offline For Now, Use This Link."

77. <http://pastebin.net/306596> contains the reason for the Salt Lake City Police Department (SLCPD) website hack. The primary motivation as mentioned at the website above was a Utah state senator's decision to introduce a bill, SB107, which addressed the possession of graffiti paraphernalia. More information on SB107 is available at <http://le.utah.gov/~2012/htmldoc/sbillhtm/sb0107.htm>.

78. <http://pastebin.net/306596> also contained a "dump" of certain parts of the SLCPD website to include the login URL as well as a list of police officers who had accounts at the website. The account information included the username, hashed password, full name, employee title, email address, and phone number. The dump contained 473 records. At the top of the post is a reference to @ItsKahuna where he claims responsibility for the hack.

79. On January 31, 2012 at 8:19 PM, @ItsKahuna posted a tweet which stated "Looking at the files I snagged from you SLCPD, it seems these files can out your confidential informants, You should up your security."

80. On February 2, 2012 at 7:33 PM, @ItsKahuna posted a tweet which stated "The person who submitted a narcotics tip to @slcpd and told them they have 3 inch penises and pea size brains. I love you bro #JustSayin."

81. Your affiant reviewed a copy of the database from the SLCPD website and found an entry which, in part, stated "You fucking pigs make me sick to my stomach seeing how you conduct your business!!! It is obvious to me cops must have 3 inch penis's and pea sized brains !!! And thats the good cops..."

82. On February 3, 2012 at 11:18 AM, @ItsKahuna posted a tweet which stated "@Amy4201 <http://t.co/HTSl2gnQ>." <http://t.co/HTSl2gnQ> redirects to <http://www.ksl.com/?nid=148&sid=19097330&pid=0>. The story index contains a link to the "Full chat with "Kahuna"." Clicking this link opens a conversation between Shara Park, a KSL reporter, and a user with the username Kahuna.

83. In the chat, Kahuna is asked to verify he is the person who hacked the SLCPD website. Kahuna responds saying he can provide a sample of the unreleased file. KSL did not post the information shared as it contained private information, but later in the chat, Kahuna provides redacted information from the database which contained a submission from the "Traffic Complaints" section of the database which included "Full Name: N---- B---" and "Email Address: -----@ldschurch.org." (Redacted to protect privacy.)

84. Your affiant reviewed a copy of the database from the SLCPD website and found an entry which matched the information provided by Kahuna. The record contained a traffic complaint from an individual whose personal information matched the pattern as described in the previous paragraph.

85. The administrator for the SLCPD website has calculated the damages accrued in responding to this hacking at just short of \$33,000.

86. The IP audit file from the Twitter search warrant return related to ItsKahuna shows five sessions being initiated with Twitter which were created on January 31, 2012 from IP address 72.240.137.223.

87. On February 2, 2012 GMT, the following conversation took place via direct message between ItsKahuna and KUTV\_EFlorez:

ItsKahuna: Do you think you could get me a recorded copy of the news broadcast from noon today :P  
KUTV\_EFlorez: We can send you the link when it gets done... Our website is down currently bc we are getting a new one but should be up ASAP.  
KUTV\_EFlorez: So just to be 110% clear you are "anonymous"?  
ItsKahuna: Yes @ anonymous

88. On February 2, 2012 GMT, the following conversation took place via direct message between ItsKahuna and AnonSikko:

AnonSikko: Saw news coverage of slcpd hack great job  
ItsKahuna: Thanks brotha, It got way more coverage than expected. This op is going flawlessly :D  
ItsKahuna: And its well covered too  
ItsKahuna: yea ive been trying to keep up with reporters all day  
ItsKahuna: lol  
AnonSikko: I'm not a fan of talking to the media but it worked  
ItsKahuna: I hate talking to them, but the slcpd was spinning it to make it false and we needed to clarify it  
AnonSikko: And a great job was done of it  
ItsKahuna: Indeed. How goes it with you?

89. On February 2, 2012 GMT, the following conversation took place via direct message between ItsKahuna and KSLSharaPark:

ItsKahuna: you around? I need to know if you can remove something from the interview the Text displayed when i disconnected and came back  
ItsKahuna: I dont want my computer host showing  
ItsKahuna: [09:44] == chattime571 [chattime57@kerpia-77F7F5D7.buckeyecom.net] has quit [Ping timeout]  
ItsKahuna: 10:09] == Kahuna [Me@kerpia-77F7F5D7.buckeyecom.net] has left #chattime []  
ItsKahuna: [10:10] == Kahuna [Me@kerpia-77F7F5D7.buckeyecom.net] has joined #chattime  
ItsKahuna: That text on <http://t.co/NcDU6pZ> this page  
KSLSharaPark: I'll send your request to our website right now.  
KSLSharaPark: Ok, I'm told it has been removed. If there is anything else that needs to go, within reason, let me know.  
ItsKahuna: Thank you, thats all. Its a long story but that couldnt be there. Thanks for taking it down :) Loved the show

90. <http://t.co/NcDU6pZ> resolves to

<http://www.ksl.com/?nid=148&sid=19097330&pid=1> and Buckeyecom.net is located in Toledo, Ohio.

91. On February 2, 2012 GMT, the following conversation took place via direct message between ItsKahuna and BenWinslow:

**ItsKahuna:** Currently this is the target of focus

**BenWinslow:** SLCPD claims only things accessible through public website were hacked. Can you confirm? Did you get into their internal system?

**ItsKahuna:** We entered their admin control panel which linked to a lot of revealing confidential information, this was a poorly designed site

**BenWinslow:** They claim to have made security changes to stop you from getting in again. Is that true?

**ItsKahuna:** I dont know, their site is still offline so i cant confirm that claim

**BenWinslow:** Thanks for talking. Keep me posted. I'll have a story up soon w/ your comments.

**ItsKahuna:** kk

**BenWinslow:** Sen. Mayne's bill just died on the Senate floor. Any comment?

**ItsKahuna:** I saw that. We are glad to see it did not pass, the law was a very unfair law using intent to commit crime as means to charge.

**BenWinslow:** So are you done with SLCPD?

**ItsKahuna:** On the issue of the bill yes, but we still want to bring awareness to their unsecure data that they should fix.

**BenWinslow:** Sen. Mayne says she will bring the bill back next year...

**ItsKahuna:** A decision that when that time comes, she will regret

#### Other Twitter direct messages

92. On November 30, 2011 at 3:49:34 PM GMT, EduardKovacs sent a direct message to ItsKahuna which stated "<http://t.co/yCOX7pX>." This URL resolves to <http://news.softpedia.com/news/Italian-and-Bhutan-Government-Websites-Hacked-by-Kahuna-237558.shtml> which outlines Kahunas hacking of Italian and Bhutan government sites.

93. On January 6, 2012 at 9:20:29 PM GMT, ItsKahuna sent a direct message to anon\_cutie which stated "anonymousecuritytestingftw@gmail.com I suppose I can give you pics soon, I dont haz micro usb cable for my phone atm at work :P."

94. On January 6, 2012 at 9:54:52 PM GMT, ItsKahuna sent a direct message to anon\_cutie which stated "time to go home from work, will be around in like an hour on anonnet if you want to stop by :)check in #doxcak3."

95. On January 6, 2012 at 10:38:00 AM GMT, ItsKahuna sent a direct message to anon\_cutie which stated "im anonJB there so you know how to find me :P." This message was in reference to ItsKahuna and anon\_cutie arranging to meet on IRC to chat.

96. On January 6, 2012 at 12:08:39 AM GMT, ItsKahuna sent a direct message to anon\_cutie which stated "Just a lil bit lol. I actually was the person who leaked the Satiagraha files with antisecc, so this is just all small stuff :P."

97. On February 19, 2012 GMT, the following conversation took place between ItsKahuna and Anomaly100:

ItsKahuna: I was never ignorant but I got really active about 8 months ago with anon, and since then have just really opened my eyes to a lot of things

ItsKahuna: going on in the world, sharing info with others, keeping informed, and helping anyway I can

ItsKahuna: heh, I actually do networking administration and server maintenance for a living, so I fix them during the day and destroy them at night :P

98. On February 21, 2012 at 8:08:19 AM GMT, ItsKahuna sent a direct message to EduardKovacs which stated "Working On #OpPiggyBank hacking police sites with CabinCr3w lately, Ive lost count of how many at this point lulz."

99. On February 19, 2012 GMT, the following conversation took place between ItsKahuna and Anomaly100:

ItsKahuna: Heading to work, will chat with you when i get there in about 30

ItsKahuna: haha they wont ever find me, im too awesome :)

ItsKahuna: Trust me, I wouldnt have gotten away with as much as I have if I wasnt careful enough to make sure I dont get caught

ItsKahuna: Im like the gingerbread man, no one can catch me :P

100. On February 25, 2012 at 1:26:27 AM GMT, ItsKahuna sent a direct message to missarahnicole which stated "Operation Payback was my first op, then I just started working in things. I've gone by other nicks before but changed when I got doxed<sup>4</sup>."

101. On February 25, 2012 at 1:34:34 AM GMT, ItsKahuna sent a direct message to missarahnicole which stated "About to turn 21 in a month." John Anthony Borell III's birthday is April 3, 1991.

102. On February 25, 2012 at 4:04:00 AM GMT, ItsKahuna sent a direct message to MissAnonFatale which stated "I'm sitting with my buddy who is an idiot and did a gram of heroin and has been puking for 6 hours. Trying to decide if hospital or not."

103. On February 25, 2012 at 10:44:40 AM GMT, ItsKahuna sent a direct message to MissAnonFatale which stated "im at my buddies house."

104. The IP audit file from the Twitter search warrant return related to ItsKahuna shows 10 sessions being initiated with Twitter which was created on 02/25/2012 between 12:07:06 AM and 9:26:27 PM GMT from IP address 72.241.1.22. Subpoena information shows this IP address was assigned to John Shaw who resides at [REDACTED] Ohio 43560-1869. Ian M. Shaw also lives at that address and has been seen picking up Borell and taking him to work at 5656 Opportunity Drive. Ian Shaw and Borell also are friends on Facebook.

b6  
b7c

105. On February 27, 2012 GMT, the following conversation took place between ItsKahuna and MissAnonFatale:

---

<sup>4</sup> "Doxed" refers to when somebody's true, personal information is revealed.



ItsKahuna: No problem. So when are you and hig getting married

MissAnonFatale: Not actually sure yet. He still needs to get a passport (halfway thru processing) & a visa into Oz yet. The last part will be easy though

106. Anonw0rmer and MissAnonFatale have claimed to be engaged on Twitter. The Houston field office has identified Anonw0rmer as Higinio O Ochoa III with Texas driver's license number 24537042. The address for Ochoa on his driver's license is [REDACTED] [REDACTED] Galveston, Texas 77551. Ochoa's date of birth is [REDACTED] Ochoa has been seen entering and exiting an apartment owned by his grandmother. The address of this apartment is [REDACTED] Galveston, TX.

b6  
b7c

107. On February 28, 2012 at 18:00:19 AM GMT, ItsKahuna sent a direct message to anon\_cutie which stated "No one has any idea who I am or what I look like, so lets keep it that way and NOT share these with anyone mkay :P <http://t.co/lhMgllL>."

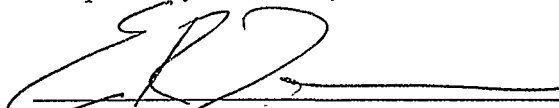
108. <http://t.co/lhMgllL> resolves to <http://imgur.com/a/MEVve> which contains two photographs, both of which match the driver's license photo for John A. Borell III.

109. Based on the forgoing, your affiant is of the opinion that there is probable cause to believe that John Anthony Borell III did knowingly transmit a program, code and information intentionally causing damage to a protected computer in violation of Title 18 United States Code, Section 1030, Fraud and Related Activity in Connection with Computers. Your affiant, therefore, respectfully requests that the attached arrest warrant be issued authorizing the arrest of the subject.

REQUEST FOR SEALING

110. I further request that the Court order that all papers in support of this application, including the affidavit and complaint, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

  
ERIC R. ZIMMERMAN

Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on March 16, 2012



PAUL M. WARNER  
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the  
District of Utah

United States of America  
v.  
JOHN ANTHONY BORELL III

Defendant

Case No.

2:12mj90PMW

FILED IN UNITED STATES DISTRICT  
COURT, DISTRICT OF UTAH  
MAR 16 2012  
D. MARK JONES, CLERK  
DEPUTY CLERK

ARREST WARRANT

To: Any authorized law enforcement officer

SEALED

**YOU ARE COMMANDED** to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) JOHN ANTHONY BORELL III

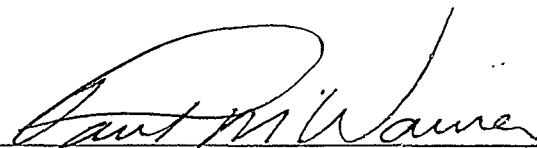
who is accused of an offense or violation based on the following document filed with the court:

- ☐ Indictment    ☐ Superseding Indictment    ☐ Information    ☐ Superseding Information    ☒ Complaint  
☐ Probation Violation Petition    ☐ Supervised Release Violation Petition    ☐ Violation Notice    ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1030; Fraud and Related Activity in Connection with Computers

Date: 16 March 2012



Issuing officer's signature

City and state: Salt Lake City, Utah

Paul M. Warner, United States Magistrate Judge

Printed name and title

Return

This warrant was received on (date) \_\_\_\_\_, and the person was arrested on (date) \_\_\_\_\_  
at (city and state) \_\_\_\_\_.

Date: \_\_\_\_\_

Arresting officer's signature

Printed name and title

DAVID B. BARLOW, United States Attorney (#13117)  
ADAM ELGGREN, Assistant United States Attorney (#11064)  
MICHAEL KENNEDY, Assistant United States Attorney (#8759)  
Attorneys for the United States of America  
185 S. State Street, Ste. 300 • Salt Lake City, Utah 84111  
Telephone: (801) 524-5682 • Facsimile: (801) 325-3387  
e-mail: adam.elggren@usdoj.gov

FILED IN UNITED STATES DISTRICT  
COURT, DISTRICT OF UTAH  
MAR 16 2012  
BY D. MARK JONES, CLERK  
DEPUTY CLERK

---

IN THE UNITED STATES DISTRICT COURT  
DISTRICT OF UTAH, CENTRAL DIVISION

---

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JOHN ANTHONY BORELL III,

Defendant.

MAGIS. NO. 2:12mj90 PMV

SEALED

COMPLAINT

SEALED

VIO. 18 U.S.C. §1030(a)(5)(A),  
FRAUD AND RELATED  
ACTIVITY IN CONNECTION  
WITH COMPUTERS

Magistrate Judge Paul M. Warner

---

Before a United States Magistrate Judge for the District of Utah, appeared  
the undersigned, who on oath deposes and says:

COUNT 1

On or about January 19, 2012, in the Central Division of the District of  
Utah,



b7E

X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXX

Total Deleted Page(s) = 64

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1514173-000

Total Deleted Page(s) = 17

Page 20 ~ Duplicate;  
Page 21 ~ Duplicate;  
Page 22 ~ Duplicate;  
Page 23 ~ Duplicate;  
Page 24 ~ Duplicate;  
Page 25 ~ Duplicate;  
Page 26 ~ Duplicate;  
Page 27 ~ Duplicate;  
Page 28 ~ Duplicate;  
Page 29 ~ Duplicate;  
Page 30 ~ Duplicate;  
Page 31 ~ Duplicate;  
Page 32 ~ Duplicate;  
Page 33 ~ Duplicate;  
Page 34 ~ Duplicate;  
Page 35 ~ Duplicate;  
Page 36 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXX



b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 16

b6  
b7C  
b7E



UNCLASSIFIED

To: Operational Technology From: Salt Lake City  
Re: [REDACTED] 02/16/2012

b7E

into a more useable format; however, the information is publically available to any visitor to Twitter.com.

UNCLASSIFIED

UNCLASSIFIED

To: Operational Technology From: Salt Lake City  
Re: [REDACTED] 02/16/2012

b7E

LEAD(s) :

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT CHANTILLY, VA

Hard copy to follow. Extract all tweets posted by  
Twitter.com userids [REDACTED] as detailed above.

b6  
b7C

♦♦

UNCLASSIFIED

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/16/2012

On February 15, 2012, SA [ ] reviewed logs from various IRC channels looking for any references to [ ]. Several other nicknames were found to include: [ ]

b6  
b7C

A search of ACS found references to [ ] in two files:

b6  
b7C  
b7E

[ ] 08/25/2011

[ ] 11/30/2011

Both serials summarize information received from someone claiming to be [ ]. Two complaints were made, one via tips.fbi.gov and one via ic3.gov. Both complaints originated from [ ] which resolves to Sprint Nextel Corporation. The complaints listed the following address and other information for [ ]

b6  
b7C

[ ]

The following is taken from the complaints filed by [ ]

b6  
b7C

[ ] reported that he is a member of [ ] goes by the nicks [ ] provided the following contact information: [ ]

[ ] reported that he has participated in numerous government agency intrusions as well as leaking classified documents. He said he was active in [ ] and has aided in the hacking of multiple individuals as well. He further claimed that he was [ ] and hosted them on his website, [ ] and had been in contact with [ ] claimed he has knowledge of the groups' inner workings and has trusted relationships with many of the members. He claimed he was tired of running and hiding.

Investigation on 02/16/2012 at Salt Lake City, Utah

File # [ ] Date dictated [ ]

b6  
b7C  
b7E

by SA [ ]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 2

[redacted]  
[redacted] is a case involving [redacted] hacking several online sites, bragging about it, and mentioning his affiliation with [redacted]. The case was opened 09/15/2011 and the last serial is dated 10/03/2011. On February 16, 2012, SA [redacted] spoke to the case agent, SA [redacted] about her case. SA [redacted] stated she will forward a copy of the log files and other information maintained in the case's 1A file for SA [redacted] to review.

b6  
b7C  
b7E

SA [redacted] reviewed the serials in [redacted]

b6  
b7C  
b7E

Serial 1 contained a link to [redacted] which is an outline of someone claiming to have hacked [redacted] Facebook page. It also contained a link to [redacted] which shows registration details for [redacted] as belonging to [redacted]

b6  
b7C

Serial 5 contains reference to the IP which the hacks originated from:

The hacking attack came from IP address 72.240.43.146, which was traced to BlessedSacramentToledo.com, a church in Toledo, Ohio, that according to Facebook, [redacted] has attended. The church is close to [redacted] residence.

b6  
b7C

The church is further identified as:

Blessed Sacrament Parish  
4227 Bellevue Road  
Toledo, Ohio 43613  
Telephone Number: 419-472-2288  
[redacted]

b6  
b7C

Serial 5 also outlines [redacted] involvement with various hacks in Brazil to include data hosted at his website [redacted]

b6  
b7C

[REDACTED]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 3

On February 16, 2012, SA [REDACTED] for  
various iterations of [REDACTED] and found the following  
information:

b6  
b7C  
b7E

[REDACTED]

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 4

[Redacted]

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 5

[Redacted]

b6  
b7C  
b7E

[REDACTED]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 6

On February 16, 2012, [REDACTED] was reviewed by SA [REDACTED] which is summarized below. The format for each post is:

b6  
b7C  
b7E

[REDACTED]

b6  
b7C  
b7E



b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 7

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 8

[Redacted]

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 9

[Redacted]

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 10

[Redacted]

b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 11

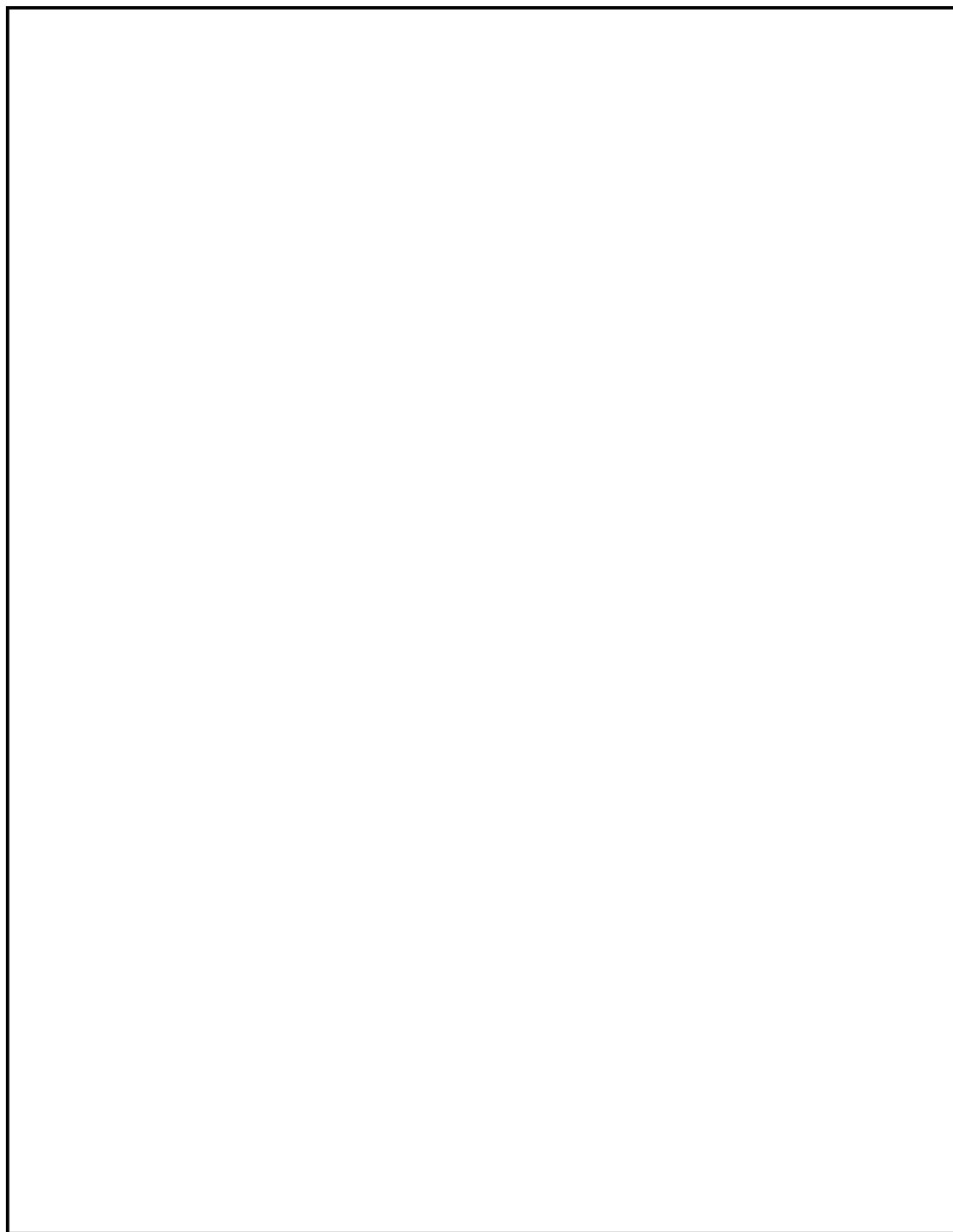
[Redacted]

b6  
b7C  
b7E

• • •

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 12



b6  
b7C  
b7E

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 13

[Redacted]

b6  
b7C  
b7E

1 2 3

[Redacted]

b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 14

[Redacted]

b6  
b7C  
b7E





b7E

Continuation of FD-302 of \_\_\_\_\_, On 02/16/2012, Page 15

b6  
b7C  
b7E

UNCLASSIFIED

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/16/2012

To: Operational Technology

Attn: UC

Investigative Analysis Unit

From: Salt Lake City

C-3

Contact: SA

Approved By:

Drafted By:

Case ID #:

Title: ANONYMOUS  
INFOBYTES - VICTIM  
www.utahchiefs.org - VICTIM;  
www.taylorsvilleut.org - VICTIM;  
CRIMINAL COMPUTER INTRUSION

**Synopsis:** To submit and request analysis of the referenced Twitter.com feed by the Operational Technology Division (OTD), Investigative Analysis Unit (IAU) regarding captioned matter.

**Details:** Investigative Analysis Unit (IAU) is requested to extract all posts (tweets) made to Twitter.com by userids [REDACTED] Please include date and time information for each tweet. Because Salt Lake City Division is requesting IAU's assistance in extracting this information, no digital media is provided.

Twitter users [REDACTED] been identified as responsible for several intrusions against various state and local police departments across the United States. They are affiliated the hacktivist group Anonymous. To date Salt Lake City has reviewed the tweets for both accounts but would like an archive of said tweets to place in the case file.

Legal Authority: The Twitter.com feed is publically available. It can be viewed by any Internet user even without logging into Twitter.com. As such, no legal process is required to view this information. IAU's assistance is need to convert the information

UNCLASSIFIED

b6  
b7C  
b7E

b6  
b7C

b6  
b7C

b6  
b7C

KSL TV KSL Newsradio iWitness

Login Feedback Contact Us

## » Utah

Enter Keyword all of KSL

Utah Page Two U.S. World Sports Weather Traffic Biz Entertainment Shows More

Classifieds Cars Homes Jobs Local Deals

Local Stories KSL 5 News Investigations Tough Times Survival Bank Staying Safe Statecraft: Government &amp; Politics Sunday Edition



**Weird Loophole in (UT):**  
If you pay more than \$9 for car insurance you better know what you're getting into.



**Salt Lake City: Mom is 52, Looks 30...**  
Her clever \$3 Wrinkle Read More

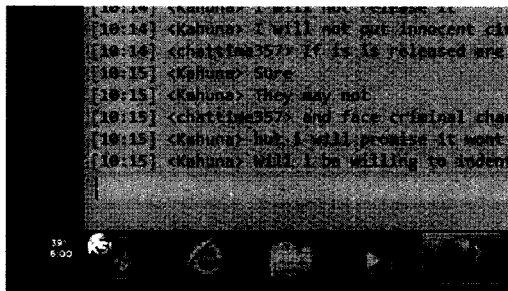


**51 year old woman looks 25**  
Salt Lake City Mom Publishes Simple \$5 Read More

About this ad

## Anonymous hacker gives details of SLCPD website hack

February 2nd, 2012 @ 1:41pm



6PM Update

5PM Update

12PM Story

### 34 Comments

Post or read comments

### Story Index

1. Main Story
2. Full Chat with "Kahuna"

### Audio

Randall Jeppesen reporting

### Related Stories

Graffiti bill fails: Rep. takes on closed-session caucuses

Personal information accessed in hack of SLCPD website

Group hacks into SLCPD website over graffiti bill

*Some sensitive material has been redacted, but the chat is otherwise unedited*

@Kahuna - SLCPD Website Hacker Chattime357 - Shara Park, KSL Reporter DCDebbie - Unknown

[09:43] <@Kahuna> Hi

[09:43] @ItsKahuna - how can we verify you are one of the hackers behind the SLCPD hack?

[09:44] <@Kahuna> I can verify with an unreleased file if you would like

[09:44] That would be a good start.

[09:45] <@Kahuna> First Name Last Name Email Last Updated (THE UNRELEASED FILE WAS REMOVED BY KSL TO PROTECT PRIVATE INFORMATION STOLEN FROM SALT LAKE CITY POLICE)

[09:46] <@Kahuna> this is a sample of their subscription records

[09:46] <@Kahuna> It has not been released

[09:46] <@Kahuna> please keep it that way

[09:47] Ok.

[09:47] <@Kahuna> Traffic Complaints SUBMISSION

[09:47] <@Kahuna> Answers on Submitted Form:

[09:47] <@Kahuna> Full Name: N---- B---

[09:47] <@Kahuna> Phone Number: xxx-xxxx

[09:47] <@Kahuna> Email Address: -----@ldschurch.org

[09:47] <@Kahuna> Complaint: After the turn light turns red, south-bound traffic continues to turn east at the intersection of State Street and South Temple. Nearly every day, pedestrians have to wait for or nearly get hit by vehicles that do not stop once the light is red. I'm confident that traffic tickets could be written every business day between 7:30 a.m. and 8:00 a.m. I'm not sure what you can/will do.

[09:47] <@Kahuna> Thanks for your consideration.

**38" JEWELRY ARMOIRE**

**ONLY... \$19<sup>99</sup>**

CLICK FOR DETAILS

With purchase \$299 or higher.

**RCWilley** **\$70 VALUE!**

ABOUT THIS AD

### Most Popular

Read Video Commented Desert News

1. Unique construction project under way at ...
2. Eric Millerberg makes initial court ...
3. Former fire captain sentenced for child ...
4. Have You Seen This? Sheep spin cycle
5. LIVE STREAM: Utah State High School ...

### Latest Videos



**Fire damages family sawdust company**  
Posted Feb 3rd - 1:16pm  
Tweet/Share



**Eric Millerberg makes initial court appearance**  
Posted Feb 3rd - 12:49pm  
Tweet/Share

**Work camp for juveniles faces closure**  
Posted Feb 3rd - 12:17pm  
Tweet/Share

b7E

[09:47] oh wow

[09:47] <@Kahuna> Traffic submission complaint

[09:47] <@Kahuna> I redacted the names and contact info

[09:47] <@Kahuna> Enough proof for you?

[09:48] We'll keep the emails out - but I'd like to use the complaint as your proof.

[09:48] <@Kahuna> Thats fine

[09:49] <@Kahuna> I have another reporter coming Emily Florez

[09:49] <@Kahuna> @KUTV\_EFlorez

[09:49] So what other info do you have? Emails are one thing - complaints are one thing - what other compromising information do you have? Just so we really know

[09:49] <@Kahuna> Wait for her to get here and then we can chat

[09:49] Emily and I are good friends - don't hack her either. :)

[09:50] <@Kahuna> chattime you are Shara Park correct?

[09:50] Correct

[09:50] <@Kahuna> Trying to figure out who im speaking with

[09:50] <@Kahuna> ok

[09:50] Are you local?

[09:50] <@Kahuna> Just one moment, trying to get another reporter her

[09:50] <@Kahuna> No i am not

[09:50] <@Kahuna> \*here

[09:51] <@Kahuna> Sorry i have a lot of press contacting me so it took a while to get responses out

[09:51] <@Kahuna> one moment

[09:51] <@Kahuna> if she isnt here in five we will continue without her

[09:53] <@Kahuna> Okay, lets talk

[09:53] <@Kahuna> i will talk to her later

[09:54] what is the motivation behind hacking of the Salt Lake Police Department?

[09:54] Ok - let's start with why SLCPD?

[09:55] <@Kahuna> This legislation based on the "Intent" to commit a crime just furthers the governmental control over the citizens of this country. It is one step further toward a full police state. We watch daily as the police listen and allow their orders to violate the rights of people

[09:55] <@Kahuna> daily we watch cops beat people, arrest them without cause, and this is a message that we are watching and that we see this as unlawful. We will be there if they carry this out

[09:56] Be there to do what?

[09:56] <@Kahuna> The foot soldiers of this corrupt government who abide by this are as much a target as the government themselves

[09:56] <@Kahuna> Whatever needs done - if they wish to arrest someone unjustly and embarrass them publicly as this will do we can assure them that everyone will know who they are

[09:56] <@Kahuna> where they live

[09:56] So are you saying you will target police officers personal information if the bill passes? I just want to be clear about that statement?

[09:56] <@Kahuna> and how to contact them

[09:57] <@Kahuna> Not just if the bill passes, but if they carry out this law and arrest people without cause based on intent

[09:57] <@Kahuna> you can be damn sure I will



**Teen ordered to remain in custody following bomb plot**  
Posted Feb 3rd - 11:37am  
Tweet/Share



**Fire forces residents to evacuate fourplex**  
Posted Feb 2nd - 8:04am  
Tweet/Share



**Naturalized citizen forced to wait 6 months for renewed license**  
Posted Feb 2nd - 10:12pm  
Tweet/Share

<< 1 2 3 4 5 6 7 8 9 10 11 12 13 >>



The secret of how to learn a foreign language in just 10 days is revealed! Read here to find out .



**Salt Lake City** - These 2 tricks allow Utah residents to get car insurance at half-price.



You can enroll in a Utah Teacher degree program. Financial Aid for those who qualify.



Can't Sleep? Try this natural solution to put your sleep problems to rest forever...

## Advertisement News

[illegible]

## Weather

[illegible]

## Traffic

$$m = \frac{1}{2} \left( \frac{1}{\alpha} + \frac{1}{\beta} \right) \quad \text{and} \quad \sigma^2 = \frac{1}{2} \left( \frac{1}{\alpha^2} + \frac{1}{\beta^2} \right)$$

## TV

[illegible]

## Sports

[illegible]

## Opinion

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$


Tweet 1

Like 67

Additional specific data on compliance with the Loan Guaranty programs and the 1972 Interagency Staff Report are available for January 1, 1973, and are reported by the Interagency Board on page 10.

\* 2011 was run by KBN Broadcasting Co. Ltd. (Co.) & Co. created & managed by Deseret Capital Media – a Deseret Media Company in 2012



Deseret Media Companies

[10:10] sorry

[10:10] what was just said

[10:10] I accidentally closed the window

[10:10] lol

[10:10] was this part of a group effort on behalf of Anonymous?

[10:11] This was part of #OpPiggyBank, a cabincr3w op

[10:11] cabincr3w works with anons

[10:12] can you please explain what the purpose of #OpPiggyBank is or do you have a link of the purpose of it is?

[10:13] Is the Salt Lake City Police Department holding back the truth from the public about what was stolen?

[10:13] They are downplaying the seriousness of the contents of the files in my opinion

[10:13] And you will not release any of the information? How can the public trust you if you were willing to steal it?

[10:14] I will not release it

[10:14] I will not put innocent civilians at risk

[10:14] If it is released are you willing to identify yourself?

[10:15] Sure

[10:15] They may not

[10:15] and face criminal charges?

[10:15] but i will promise it wont

[10:15] Will i be willing to identify myself? No

[10:16] what purpose would i have to agreeing to that if you dont wish to take my word for it that is your choice

[10:16] but they wont be released

[10:16] Looks like we will have to

[10:17] How did you find out about the bill if you are not local?

[10:17] I assure you, and i cannot hesitate, innocent civilians reporting crimes are not my target

[10:17] i would not put their lives in danger

[10:17] how did i find out? the internet is a vast place, i stay educated on events all over the country

[10:18] What do you want people to know - people who feel violated by what you have done?

[10:19] To the citizens: Nothing in this is a target to you, we are not out to cause you any harm nor would we ever do so, this is targetted at unjust lawmakers and those who enforce there unjust laws

[10:19] to the police and lawmakers, if this bill continues and passes and causes a single arrest of intent, this wont be the only time that they hear from us, and they better expect us

[10:19] Well I can say this is a first for me, chatting with a hacker

[10:20] i laughed at your #Pleasedonthack me hashtag

[10:20] made my morning :D

[10:20] Oh good, but seriously please dont. :)

[10:20] lol i wont :P

**Shara Park:** Email: [spark@ksl.com](mailto:spark@ksl.com) Twitter: [@KSLSharaPark](https://twitter.com/KSLSharaPark)  
**Randall Jeppesen:** Email: [rjeppesen@ksl.com](mailto:rjeppesen@ksl.com) Twitter: [@RJENEWS](https://twitter.com/RJENEWS)

Advertisement

## Site Index

[09:58] <@Kahuna> This bill opens up a large door to allowing arrest without a crime being committed

[09:58] <@Kahuna> you cannot charge someone because you think they had an intent to commit a crime

[09:59] By doing that you will be putting them at risk on so many levels - not with just exposing their personal information but physically as well? There are a lot of people out there that want to hurt police officers.

[09:59] <@Kahuna> For something as small ass possession of a legal item

[09:59] Sorry if you don't mind me asking, what is the specific law that is planning to be passed?

[09:59] <@Kahuna> SB107

[09:59] <@Kahuna> The polic cannot violate the rights of the people and think that we will not act and show them that it is not acceptable

[10:00] Lets talk about the information you gathered - describe for me where it comes from? What agencies?

[10:00] <@Kahuna> The information all comes from the SLCPD

[10:01] I apologize is it the Utah bill - Possession of Graffiti Paraphernalia?

[10:01] <@Kahuna> YEs

[10:01] Right - but is it just citizen complaints? Or are their documents that could compromise investigations?

[10:01] Are there - sorry

[10:02] <@Kahuna> Chattime, there are details into suppliers, names, license plate numbers, locations, warrant numbers, times

[10:02] <@Kahuna> For drug operations

[10:02] <@Kahuna> how that affects an investigation is outside of my scope of knowledge i am not a police officer and do not know how their investigations in salt lake city function

[10:02] How many documents total?

[10:02] <@Kahuna> let me check my computer

[10:04] but do you fear that existing investigations may be affected due to this hacking incident?

[10:04] <@Kahuna> 643 narcotic operation related documents, 2042 job application documents 77 police contact requests, 228 traffic complaint related documents, and numerous subscription info

[10:04] <@Kahuna> We will not be releasing the documents, no investigations will be affected

[10:04] <@Kahuna> I am the only person with a copy

[10:05] for example tips of violent crimes such as murder, rape? which can lead to the arrest of dangerous individuals?

[10:05] <@Kahuna> I have not looked through the documents, but they seem all drug operation related

[10:05] <@Kahuna> though i am sure many of these people are violent criminals involved in this

[10:05] <@Kahuna> Which is why we wont be releasing

[10:06] So were you able to gather these documents directly from their website, or was their website a portal to a server?

[10:06] <@Kahuna> It was accesible with their admin logins

[10:06] <@Kahuna> though the passwords were secured using sha1 it was not hard to get around

[10:06] So just to follow - you were able to hack their site, gain log in info, then access the info on their private site.

[10:07] <@Kahuna> Yes, hacked the site, got their logins from their database, broke the admin passwords sha1 hash

[10:07] <@Kahuna> and then accessed their admin panel

[10:07] <@Kahuna> where i took all their files from

[10:09] was this part of a group effort on behalf of Anonymous?

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1514173-000

Total Deleted Page(s) = 2  
Page 8 ~ b6; b7C; b7D; b7E;  
Page 9 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXX



UNCLASSIFIED

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/31/2012

To: Salt Lake City

Attn: Cyber

From: Salt Lake City

C3

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

Title: CHANGED  
ANONYMOUS  
INFOBYTES - VICTIM  
www.utahchiefs.org - VICTIM  
www.taylorsvilleut.org - VICTIM  
CRIMINAL COMPUTER INTRUSION

Synopsis: To add another victim to case file, www.slcpd.com

Previous Title: Title marked "Changed" to reflect ANONYMOUS  
INFOBYTES - VICTIM  
www.utahchiefs.org - VICTIM  
www.taylorsvilleut.org - VICTIM  
www.slcpd.com - VICTIM  
CRIMINAL COMPUTER INTRUSION.

Title previously carried as "ANONYMOUS  
INFOBYTES - VICTIM  
www.utahchiefs.org - VICTIM  
www.taylorsvilleut.org - ." VICTIM  
CRIMINAL COMPUTER INTRUSION

Details: On 1/31/2012, at approximately 3:00 p.m., FBI Seattle  
IA [REDACTED] contacted SA [REDACTED] via telephone to  
notify him that a Seattle CHS [REDACTED]

[REDACTED]

b6  
b7C  
b7E

b6  
b7C  
b7D  
b7E

UNCLASSIFIED

031 [REDACTED] 102.ec

b6  
b7C

UNCLASSIFIED

b7E

To: Salt Lake City From: Salt Lake City  
Re: [REDACTED] 01/31/2012

SA [REDACTED] notified ASAC Ken Porter regarding the initial report of the Salt Lake City Police Department's website being compromised. ASAC Porter notified Deputy Chief Terry Fritz of the compromised website and that the subjects were anonymous.

b6  
b7C

FBI Seattle SA [REDACTED] contacted SA [REDACTED] and advised she has the website where Anonymous announced they compromised the [www.slcpd.com](http://www.slcpd.com) website. The website was located at: <http://pastebin.com/raw.php?i=tpit8bD3>

b6  
b7C

Partial content of the website is pasted below and the actual user names, hashed passwords, employee title, email, and telephone number are saved to a compact disk and placed in a 1a envelope located in this case file.

\*\*\*\*\*

[REDACTED]

b6  
b7C

=====

[REDACTED]  
@CabinCr3w & [REDACTED]

=====

Dear Salt Lake City Police Department,

We took note <http://fur.ly/0/MaynePlot> that Senator Karen Mayne has put forth a bill SB107 - <http://fur.ly/0/MaynePlotBill> that tries to resolve an inconvenience with a flamethrower. Regardless whether the messages spray painted are disturbing, this bill sets an attitude that will down the line lead to invasions of privacy in people's homes and raids at 6 am over spray paint. We know that law enforcement functions as a mindless machine led by InfraGard, PERF, and other domestic civil intelligence (so marches the security state) networks. We know there's money to be made in the "just doing my job" compartmentalized economy. Therefore we know that regardless of the intent of Karen Mayne's haphazard lawmaking, this will end in corporations selling miniature drones to police officers chasing 13 year olds. We will act now as we have seen other "well-meaning" legislation open the door to tyranny and financing of oppression. There is no denying where this will end in 3 to 5 years or perhaps sooner.

Has your Senator Karen Mayne watched Minority Report too many times? A law prohibiting ownership and use of purchased products based on suspected intent?

UNCLASSIFIED

**From:** [redacted] (OC) (FBI)  
**Sent:** Friday, February 03, 2012 12:59 PM  
**To:** [redacted] (OC) (FBI); [redacted] (SU) (FBI)  
**Subject:** RE: Twitter Reporting

b6  
b7C

Classification: UNCLASSIFIED//~~FOUO~~  
=====

[redacted]

**From:** [redacted] (OC) (FBI)  
**Sent:** Friday, February 03, 2012 1:56 PM  
**To:** [redacted] (SU) (FBI)  
**Subject:** Twitter Reporting

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~  
=====

<< File: 20120201.docx >>

SA [redacted]

Tulsa RA - Squad 11

[redacted] Office  
[redacted] Blackberry

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED

b7E

To: Salt Lake City From: Salt Lake City  
Re: [REDACTED] 01/31/2012

[REDACTED] Web Developer 1, showed SA [REDACTED] and FE [REDACTED] the website logs and .php pages that are used to populate the [www.slcpd.com](http://www.slcpd.com) website. [REDACTED] contacted former Web Developer 2, [REDACTED] telephone number [REDACTED] who was once an Salt Lake City employee responsible for the [www.slcpd.com](http://www.slcpd.com) back end database. [REDACTED] advised that when he was notified by [REDACTED] about the intrusion he logged into the [www.slcpd.com](http://www.slcpd.com) database and [REDACTED]

b6  
b7C  
b7E

also observed that the attackers utilized his username and guessed his password, which was [REDACTED] to access the website and add content to the website. He said there were three pages created by the attackers that reflected his name to indicate again they used his credentials to log into the website.

[REDACTED]  
[REDACTED] once they logged on with his credentials. [REDACTED] advised that [REDACTED]  
[REDACTED] recommended [REDACTED]  
[REDACTED] He stated that approximately six to eight months ago he noticed the following IP addresses attempting to log into the website administration console:

b6  
b7C  
b7E

[REDACTED] resolved to the United Kingdom  
[REDACTED] resolved to Lehi, Utah  
[REDACTED], resolved to Ireland

b6  
b7C

[REDACTED] stated that [REDACTED]  
[REDACTED]  
[REDACTED] stated that he is no longer employed by Salt Lake City, but he is available to assist in this investigation.

b6  
b7C  
b7E

♦♦

UNCLASSIFIED

**RE: Twitter Reporting**

[redacted] (OC) (FBI)

**Sent:** Monday, February 06, 2012 5:21 PM

**To:** [redacted] (SU) (FBI)

**Cc:** [redacted] (OC)(FBI)

b6  
b7C

Classification: UNCLASSIFIED//~~FOUO~~

[redacted]

Our CHS has identified [redacted] I will have the [redacted] written up today, but it may be late (I'll send you a draft). Our CHS was unable to find much on [redacted]

b3  
b6  
b7C  
b7D  
b7E

[redacted] (cc'd) has sent a preservation letter to [redacted]  
[redacted] We're ok with SLC pursuing search warrants for either [redacted] as the crime is definitely yours.  
[redacted] is pursuing a GJ subpoena for [redacted] at this time. We'll add you to our Rule 6e list and provide you with the results of that subpoena.

Thanks

[redacted]

**From:** [redacted] (SU) (FBI)

**Sent:** Monday, February 06, 2012 12:29 PM

**To:** [redacted] (OC) (FBI)

**Subject:** RE: Twitter Reporting

b6  
b7C

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] seems to be one of the leaders. I assume he is CONUS? Is he one of the ones you are interested in? my primary target is [redacted]

b5  
b6  
b7C

[redacted]

**From:** [redacted] (OC) (FBI)

**Sent:** Monday, February 06, 2012 7:50 AM

**To:** [redacted] (SU) (FBI)

**Subject:** RE: Twitter Reporting

b6  
b7C

Classification: UNCLASSIFIED//~~FOUO~~

b7E

2/6/2012

=====

b6  
b7C

Our guy says he got the true name and location of  We're meeting this afternoon, and I'll provide you details before COB today.

Thanks

**From:** (SU) (FBI)**Sent:** Friday, February 03, 2012 2:25 PM**To:** (OC) (FBI)**Subject:** RE: Twitter Reportingb6  
b7CClassification: UNCLASSIFIED//~~FOUO~~

=====

Thanks for the call. That is some good info!

I am interested in any and all information on  to include:b5  
b6  
b7C  
b7E seems to know  at some level based on posts from  to  on twitter.

OTHER

 The slcpd case is huge right now and everyone from my SAC to the governor of Utah is involved.

Again, many thanks.

2/6/2012

b7E

UNCLASSIFIED

b7E

To: Salt Lake City From: Salt Lake City  
Re: [REDACTED] 01/31/2012

Is she kidding? The purpose of the law is not to prevent crime, but to manage it. The public gets the benefit of the doubt. A little too zealous wethinks. Perhaps a little pre-emptive action will drive the point home. As the foot soldiers for this bill, you get a taste of Mayne's witch hunt mentality. There are plenty of means to prosecute defacement of both private and public property in a general way. There's also the fact that some of this behavior may fall under civil rather criminal context.

A felony has a serious effect on a person's liberties after serving sentences, including loss of second amendment rights. And is this really the way to handle it? Perhaps Karen Mayne should be looking into why your neighborhoods are drawing this kind of behavior? Not acknowledging grievances and social issues such as poverty can lead to communities forming their own identities separate from their leaders. If all the senator has to offer is a policy that will lead to a self-righteous escalation of enforcement, consider this our deterrent.

We are Anonymous  
We are Legion  
We do not forgive  
We do not forget  
Expect us

```
+=====+
|         -Target-         |
|   http://www.slcpd.com   |
|   Salt Lake City PD     |
|                           |
|   Login Page             |
| http://www.slcpd.com/login.php |
+=====+
```

At 6:30 p.m. Intermountain West Regional Computer Forensic Lab Forensic Examiner [REDACTED] contacted [REDACTED] and requested his presence at the Salt Lake City Police Department to meet with Deputy Chief Michael R. Brown, Lieutenant [REDACTED] Web Developer 1, [REDACTED] to discuss the recent compromise of the www.slcpd.com website.

b6  
b7C

SA [REDACTED] conducted a [REDACTED]  
[REDACTED]

b6  
b7C  
b7E

UNCLASSIFIED